Advanced Theorem Proving Techniques in PVS And Applications

César A. Muñoz

NASA Langley Research Center Cesar.A.Munoz@nasa.gov



Objective

- Provide a gentle introduction to advanced features of the Prototype Verification System (PVS), including: theory interpretations, real number proving, implicit induction, batch proving, rapid prototyping, and strategy development.
- Illustrate these features with examples taken from verification research at NASA.



Syllabus

Lecture 1 PVS for the Impatient.

Lecture 2 Recursion, Induction, and Other Demons.

Lecture 3 \mathbb{R} eal Applications.

Concluding Remarks

Formal Methods in NextGen:

- ► NextGen is a system of systems: aircraft, physical environment, human operators.
- Formal methods for system engineering rather than for software engineering.
- Different sources of uncertainty.
- ► Highly distributed safety critical systems.

Practical Challenges

- Evolutionary vs. revolutionary concepts.
- ► Theoretical vs. practical solutions.
- ► Local vs. global solutions.

Current Technical Challenges

Automation, automation:

- ▶ Non-linear arithmetic.
- ▶ Floating point arithmetic.
- Probabilistic reasoning.

Why Higher-Order Logic Theorem Proving

- ► Higher-order logic is a general specification language that supports a variety of specification styles: axiomatic, declarative, functional, executable, etc.
- ▶ Domain of interest involves physical environment (continuous models) and digital systems (discrete behavior).
- ► Formal verification of high-level concepts/algorithms.

Why PVS?

- Pragmatic Verification System: Rich specification language that is close to a functional programming language and powerful theorem prover.
- ► Why Not?

Coming Soon

- ▶ PVS to Java code generator.
- Termination analysis tool.
- Dimensional type checking.
- ▶ Interval analysis with Bernstein polynomials.
- ► Fourth NASA Formal Methods Symposium (NFM 2012): http://shemesh.larc.nasa.gov/nfm2012.

References

- ▶ PVS: http://pvs.csl.sri.com.
- ► NASA PVS Libraries: http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html.
- ► PVS research sponsored by NASA: http://shemesh.larc.nasa.gov/fm/fm-pvs.html.
- ► Formal methods research at NASA: http: //shemesh.larc.nasa.gov/fm/fm-main-research.html.
- ► Advanced Theorem Proving Techniques in PVS and Applications:
 - http://shemesh.larc.nasa.gov/people/cam/LASER2011.